# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-294120
(43)Date of publication of application : 11.11.1997

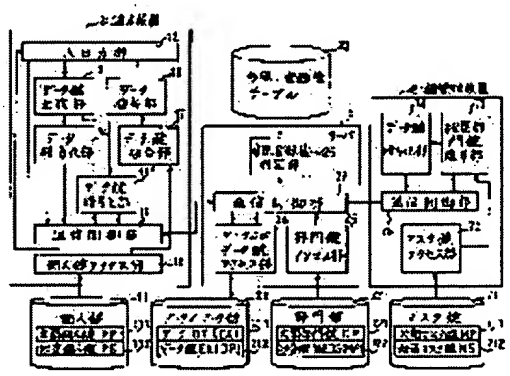
(51)Int.Cl. H04L 9/08
G09C 1/00
H04L 9/14

(21)Application number : 08-107501
(22)Date of filing : 26.04.1996

(71)Applicant : HITACHI LTD
(72)Inventor : SATO MAKOTO
NANBA AKIRA
DOMYO SEIICHI
TAKARAGI KAZUO
SHIBAHARA SETSUO

## (54) ACCESS CONTROL METHOD AND SYSTEM FOR CIPHERED SHARED DATA

(57)Abstract:
PROBLEM TO BE SOLVED: To allow user groups to share data with security by using a ciphering communication technology.
SOLUTION: A data ciphering section 14 and a data key ciphering section 15 of a terminal equipment 3 cipher data respectively by using a data key generated by a data key generating section 13 and use a public key 221 corresponding to a designated secrecy group to cipher the data key and a server 5 stores the data 211 and a data key 212. In the case of referencing the data 211, the terminal equipment 3 sends the acquired data key 212 and an open individual key 111 to the server 5, the server 5 uses a secret key to decode the data key 212 and uses the open individual key 111 to cipher the decoded data key and sends the result to the terminal equipment 3. A data key decoding section 17 uses a secret individual key 112 to decode the acquired data key and a data decoding section 18 decodes the data.



LEGAL STATUS

[Date of request for examination] 18.02.2003

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

**特開平9－294120**

(43)公開日　平成９年(1997)11月11日

| (51)Int.Cl.[6] | | 識別記号 | 庁内整理番号 | Ｆ Ｉ | | 技術表示箇所 |
|---|---|---|---|---|---|---|
| Ｈ０４Ｌ | 9/08 | | | Ｈ０４Ｌ | 9/00 | ６０１Ｂ |
| Ｇ０９Ｃ | 1/00 | ６３０ | 7259－5Ｊ | Ｇ０９Ｃ | 1/00 | ６３０Ｂ |
| | | | 7259－5Ｊ | | | ６３０Ｅ |
| Ｈ０４Ｌ | 9/14 | | | Ｈ０４Ｌ | 9/00 | ６０１Ｅ |
| | | | | | | ６４１ |

審査請求　未請求　請求項の数５　ＯＬ　（全９頁）

(21)出願番号　特願平8－107501

(22)出願日　平成８年(1996)４月26日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　佐藤　真
東京都江東区新砂一丁目６番27号　株式会社日立製作所公共情報事業部内

(72)発明者　難波　電
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(72)発明者　道明　誠一
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(74)代理人　弁理士　高橋　明夫

最終頁に続く

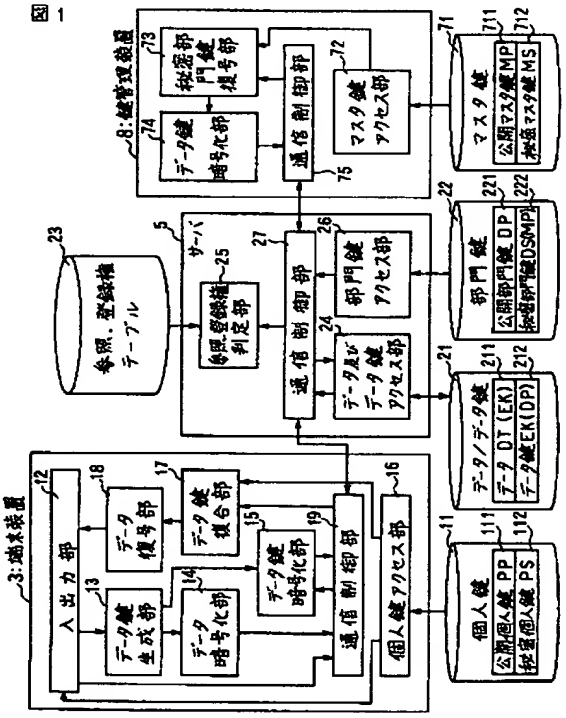
(54)【発明の名称】　暗号化された共有データのアクセス制御方法及びシステム

(57)【要約】

【課題】　暗号化通信技術を用いてユーザグループの間で安全にデータを共有する。

【解決手段】　端末装置３のデータ暗号化部１４及びデータ鍵暗号化部１５は、それぞれデータ鍵生成部１３が生成したデータ鍵によってデータを暗号化し、指定された機密区分に対応する公開部門鍵２２１を用いてデータ鍵を暗号化し、サーバ５にデータ２１１及びデータ鍵２１２を格納する。データ２１１を参照するとき、端末装置３は取得したデータ鍵２１２及び公開個人鍵１１１をサーバ５へ送信し、サーバ５は鍵管理装置８を介して秘密マスタ鍵７１２によって秘密部門鍵２２２、秘密部門鍵によってデータ鍵２１２を復号し、公開個人鍵１１１を用いて復号されたデータ鍵を暗号化して端末装置３へ送信する。データ鍵復号部１７は秘密個人鍵１１２を用いて取得したデータ鍵を復号し、データ復号部１８がデータを復号する。

図１



1

【特許請求の範囲】

【請求項１】公開個人鍵と対応する秘密個人鍵とを保持する複数の端末装置と、機密区分の各レベルに対応して公開部門鍵とそれぞれ対応する秘密部門鍵とを保持するサーバとがネットワークによって接続されるシステムのアクセス制御方法であって、

端末装置によってデータ鍵を生成し、該データ鍵を用いてデータを暗号化し、指定された機密区分に対応する公開部門鍵を用いて該データ鍵を暗号化し、暗号化されたデータとデータ鍵とを該サーバへ送信し、

該サーバによって該データと該データ鍵とを共有データとして記憶装置に格納し、

端末装置によって該サーバから該データと該データ鍵とを取得し、公開個人鍵と受け取った該データ鍵とを該サーバへ送信し、

該サーバによって該秘密部門鍵を用いて該データ鍵を復号し、該公開個人鍵を用いて復号したデータ鍵を暗号化して該端末装置へ送信し、

該端末装置によって秘密個人鍵を用いて該データ鍵を復号し、復号したデータ鍵によって取得した該データを復号することを特徴とする暗号化された共有データのアクセス制御方法。

【請求項２】該端末装置によって該データと該データ鍵とを取得する前に、該サーバによってユーザが属するユーザグループと該ユーザグループに許可されるデータ参照の機密区分とから該データを参照する権限の有無を判定することを特徴とする請求項１記載の暗号化された共有データのアクセス制御方法。

【請求項３】さらに該端末装置によって該サーバから該データ鍵を取得し、受け取った該データ鍵と変更後の機密区分とを該サーバへ送信し、

該サーバによって該秘密部門鍵を用いて受け取った該データ鍵を復号し、指定された機密区分に対応する公開部門鍵によって復号したデータ鍵を暗号化し、該記憶装置に格納される元の該データ鍵を変更後の暗号化したデータ鍵によって更新することを特徴とする請求項１記載の暗号化された共有データのアクセス制御方法。

【請求項４】公開個人鍵と対応する秘密個人鍵とを保持する複数の端末装置と、機密区分の各レベルに対応して公開部門鍵とそれぞれ対応する秘密部門鍵とを保持するサーバとがネットワークによって接続されるシステムのアクセス制御方法であって、

端末装置によってデータ鍵を生成し、該データ鍵を用いてデータを暗号化し指定された機密区分に対応する公開部門鍵を用いて該データ鍵を暗号化し、暗号化されたデータとデータ鍵とを該サーバへ送信し、

該サーバによって該データと該データ鍵とを共有データとして記憶装置に格納し、

端末装置によって該サーバから該データと該データ鍵とを取得し、公開個人鍵と受け取った該データ鍵とを該サーバへ送信し、

該サーバに接続される鍵管理装置によって該秘密部門鍵を用いて該データ鍵を復号し、該公開個人鍵を用いて復号したデータ鍵を暗号化して該サーバを経由して該端末装置へ送信し、

該端末装置によって秘密個人鍵を用いて該データ鍵を復号し、復号したデータ鍵によって取得した該データを復号することを特徴とする暗号化された共有データのアクセス制御方法。

【請求項５】公開個人鍵と対応する秘密個人鍵とを保持する複数の端末装置と、機密区分の各レベルに対応して公開部門鍵とそれぞれ対応する秘密部門鍵とを保持するサーバとがネットワークによって接続されるアクセス制御システムであって、

該端末装置は、データ鍵を生成し、該データ鍵を用いてデータを暗号化し指定された機密区分に対応する公開部門鍵を用いて該データ鍵を暗号化し、暗号化されたデータとデータ鍵とを該サーバへ送信する手段と、該サーバから該データと該データ鍵とを取得し、公開個人鍵と受け取った該データ鍵とを該サーバへ送信する手段とを有し、

該サーバは、該データと該データ鍵とを共有データとして記憶装置に格納する手段と、該秘密部門鍵を用いて該データ鍵を復号し、該公開個人鍵を用いて復号したデータ鍵を暗号化して該端末装置へ送信する手段とを有し、

該端末装置は、さらに秘密個人鍵を用いて受信した該データ鍵を復号し、復号したデータ鍵によって取得した該データを復号する手段を有することを特徴とする暗号化された共有データのアクセス制御システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、暗号化されたデータのアクセス制御方法に係わり、特に暗号化されたデータを同一のアクセス権をもったユーザの間で共有するときのアクセス制御方法に関する。

【０００２】

【従来の技術】端末装置とサーバ装置との間で暗号通信する方法として、例えば特開平３－２４３０３５号公報は、共通鍵暗号方式に従ってデータをデータ鍵によって暗号化し、データ鍵を公開鍵暗号方式の公開鍵によって暗号化して送信する暗号通信システムを開示する。データの暗号化と復号には同一のデータ鍵を用いるためにデータの暗号化と復号処理が高速に行われる。

【０００３】図８は、上記暗号通信システムの構成を示す図である。各端末装置９０は、ユーザの数だけの公開個人鍵ＰＰ１，ＰＰ２，・・・と端末ごとの秘密鍵ＴＳ１，ＴＳ２，・・・を保持する。サーバ９１は、端末対応の公開鍵ＴＰ１，ＴＰ２，・・・とユーザの数だけの秘密個人鍵ＰＳ１，ＰＳ２，・・・を保持する。鍵管理装置９２は、公開マスタ鍵ＭＰ及び秘密マスタ鍵ＭＳを

保持する。秘密個人鍵は、公開マスタ鍵ＭＰによって暗号化されている。図中で記号Ｘ（Ｙ）は、対象Ｘが鍵Ｙによって暗号化されていることを示す。対象Ｘはデータ、データ鍵、秘密個人鍵などである。端末装置９０からサーバ９１を利用するユーザ１に対して暗号通信するときには、端末装置９０で発生させたデータ鍵ＥＫをユーザ１の公開個人鍵ＰＰ１によって暗号化してＥＫ（ＰＰ１）となったデータ鍵をサーバ９１へ送信する。サーバ９１にはユーザ１だけがアクセス権を有する領域に秘密個人鍵ＰＳ１（ＭＰ）が保持されているので、ユーザ１はこの秘密個人鍵ＰＳ１（ＭＰ）にアクセスし、サーバ９１及び鍵管理装置９２がＰＳ１（ＭＰ）を復号した後の秘密個人鍵ＰＳ１を用いてデータ鍵ＥＫ（ＰＰ１）を復号し、得られたデータ鍵ＥＫによって端末装置９０からサーバ９１へ送られたデータＤＴ（ＥＫ）を復号することができる。サーバ９１から端末装置９０に暗号通信するときには、サーバ９１で発生させたデータ鍵ＥＫを端末の公開鍵ＴＰ１によって暗号化してＥＫ（ＴＰ１）となったデータ鍵を端末装置９０へ送信する。端末装置９０では秘密鍵ＴＳ１を用いてデータ鍵ＥＫ（ＴＰ１）を復号し、得られたデータ鍵ＥＫによってサーバ９１から端末装置９０へ送られたデータＤＴ（ＥＫ）を復号することができる。鍵管理装置９２は外部から読み出すことができない公開マスタ鍵ＭＰによって秘密個人鍵ＰＳを暗号化し、秘密マスタ鍵ＭＳによって秘密個人鍵ＰＳ（ＭＰ）を復号する。

【０００４】

【発明が解決しようとする課題】上記従来技術は、暗号通信技術を使って安全にデータの登録と参照を可能とするが、暗号通信は個人対個人の通信に限られており、同一のデータ参照権を有するユーザグループの間でデータを共有するという考え方は見当らない。一方機密性が求められるデータを共有する技術として、強制アクセス制御と呼ばれる技術が知られているが、この技術は特別なオペレーティングシステムによる制御が必要とされ、特定の計算機ハードウェア及びオペレーティングシステムの下でなければ利用できなかった。特別なハードウェアやオペレーティングシステムを導入することなく、安全性の高い暗号通信技術を利用して機密性のあるデータをユーザグループの間で共有する技術が望まれている。

【０００５】本発明の目的は、暗号化されたデータをユーザグループの間で安全に共有するアクセス制御方法を提供することにある。

【０００６】

【課題を解決するための手段】本発明は、複数の端末装置とサーバ装置とがネットワークによって接続されるシステムのアクセス制御方法であって、端末装置側に公開個人鍵と対応する秘密個人鍵とを保持し、サーバ側に機密区分の各レベルに対応して公開部門鍵とそれぞれ対応する秘密部門鍵とを保持する。端末装置では共通鍵暗号方式に従ってデータを暗号化し、指定された機密区分に対応する公開部門鍵を用いてデータ鍵を暗号化して、暗号化されたデータとデータ鍵とをサーバへ送信し、サーバによって記憶装置に格納する。サーバに格納された共有データをアクセスするときには、端末装置によってサーバからデータとデータ鍵とを取得し、公開個人鍵と受け取ったデータ鍵とをサーバへ送信し、サーバによって秘密部門鍵を用いてデータ鍵を復号し、公開個人鍵を用いて復号したデータ鍵を暗号化して端末装置へ送信し、端末装置によって秘密個人鍵を用いてデータ鍵を復号し、復号したデータ鍵によって取得したデータを復号する。

【０００７】

【発明の実施の形態】以下、本発明のアクセス制御システムの一実施形態について図面を用いて説明する。

【０００８】図１は、本実施形態のシステムの構成図である。端末装置３はデータを入力及び出力する装置である。サーバ５は入力されたデータ及びデータ鍵を格納するとともに、データの機密区分に従って部門鍵（ドメインの鍵）を格納する装置である。鍵管理装置８は、部門鍵を復号するためのマスタ鍵を格納し、秘密マスタ鍵によって部門鍵を復号する装置である。本実施形態では、データの暗号化／復号にはともに同一の鍵を用いる共通鍵暗号方式を適用する。またデータを暗号化するときの鍵であるデータ鍵の暗号化／復号にはそれぞれ異なる鍵を用いる公開鍵暗号方式を適用する。

【０００９】端末装置３に接続される記憶装置１１は、個人鍵として公開個人鍵１１１と秘密個人鍵１１２とを格納する。入出力部１２は図示しないキーボード／表示装置／記憶装置のような入出力装置からのデータの入出力を制御する制御部である。データ鍵生成部１３は、共通鍵暗号方式に従ってデータ鍵を生成する処理部である。データ暗号化部１４は、共通鍵暗号方式に従って入力されたデータを生成されたデータ鍵によって暗号化する処理部である。データ鍵暗号化部１５は、公開鍵暗号方式に従って生成されたデータ鍵を公開部門鍵２２１によって暗号化する処理部である。個人鍵アクセス部１６は、記憶装置１１の個人鍵へのアクセスを制御する制御部である。データ鍵復号部１７は、公開鍵暗号方式に従ってサーバ５から受け取ったデータ鍵を秘密個人鍵１１２によって復号する処理部である。データ復号部１８は、共通鍵暗号方式に従って復号されたデータ鍵によってデータを復号する処理部である。通信制御部１９は、ネットワークを介して端末装置３とサーバ５との間に公開部門鍵２２１、データ２１１、データ鍵２１２及び公開個人鍵１１１を送受信するよう制御する制御部である。なお端末装置３にはこの他に個人鍵を生成する処理部が存在する。

【００１０】サーバ５に接続される記憶装置２１は、データ２１１及びデータ鍵２１２を格納する。データ２１

１は共通鍵暗号方式に従ってデータ鍵ＥＫによって暗号化された状態で格納され、データ鍵２１２は公開鍵暗号方式に従って公開部門鍵２２１によって暗号化された状態で格納される。また記憶装置２２は、部門鍵として公開部門鍵２２１及び秘密部門鍵２２２を格納する。秘密部門鍵２２２は公開鍵暗号方式に従って公開マスタ鍵７１１で暗号化された状態で格納される。参照・登録権テーブル２３は、各ユーザのグループについてデータ参照時及びデータ登録時の機密区分のレベルを登録するものであり、サーバ５に接続される記憶装置上に格納される。データ及びデータ鍵アクセス部２４は、記憶装置２１上のデータ２１１及びデータ鍵２１２へのアクセスを制御する制御部である。部門鍵アクセス部２６は、記憶装置２２上の部門鍵へのアクセスを制御する制御部である。参照・登録権判定部２５は、参照・登録権テーブル２３を参照して各ユーザが要求するデータ参照及び登録が妥当か否かを判定する処理部である。通信制御部２７は、ネットワークを介して端末装置３との間の通信を制御するほかに、ネットワークを介して鍵管理装置８との間に公開個人鍵１１１、データ鍵及び秘密部門鍵２２２を送受信するよう制御する制御部である。なおサーバ５には端末装置３を利用するユーザに通常のサービスを提供するモードと、通常のサービスを停止してサーバ５の記憶装置２２上の部門鍵を更新するメンテナンスモードとの２つのモードがある。サーバ５がメンテナンスモードのときには、図示しない部門鍵を更新する処理部が動作し、図示しない入出力部から入力されるデータに従って部門鍵を更新する。

【００１１】鍵管理装置８に接続される記憶装置７１は、マスタ鍵として公開マスタ鍵７１１及び秘密マスタ鍵７１２を格納する。マスタ鍵アクセス部７２は、記憶装置７１上のマスタ鍵へのアクセスを制御する制御部である。秘密部門鍵復号部７３は、公開鍵暗号方式に従って秘密マスタ鍵７１２により秘密部門鍵２２２を復号し、復号された秘密部門鍵によってデータ鍵２１２を復号する処理部である。データ鍵暗号化部７４は、復号されたデータ鍵を公開個人鍵１１１によって暗号化する処理部である。通信制御部７５は、ネットワークを介して通信制御部２７との間の通信を制御する制御部である。なお鍵管理装置８には通常のサービスを提供するモードと、記憶装置７１上のマスタ鍵を更新するメンテナンスモードとの２つのモードがあるが、サーバ５と鍵管理装置８とは同時には同じモードでなければならない。鍵管理装置８がメンテナンスモードのときには、図示しないマスタ鍵を更新する処理部が動作し、鍵管理装置８内の図示しない入出力部から入力されるデータに従ってマスタ鍵を更新する。

【００１２】端末装置３、サーバ５及び鍵管理装置８は、例えばパソコンのような情報処理装置であり、各制御部及び処理部はハードウェアによって又はこの情報処



理装置の記憶装置に格納するプログラムを実行することによって実現される。

【００１３】図２は、データをデータ鍵によって暗号化し、暗号化されたデータとデータ鍵を記憶装置２１に格納するまでの端末装置３及びサーバ５の処理の流れを示すフローチャートである。端末装置３の入出力部１２は、例えばファイルのようにまとまったデータとその機密区分を入力する（ステップ３１）。データ鍵生成部１３は、データ鍵ＥＫを生成する（ステップ３２）。データ鍵は乱数、日付等を種データとしてこれから生成される。次にデータ暗号化部１４は入力されたデータを生成されたデータ鍵によって暗号化する（ステップ３３）。次にデータ鍵暗号化部１５は、通信制御部１９を介してサーバ５へ公開部門鍵の送信要求を送信する（ステップ３４）。この送信要求は機密区分の指定を含んでいる。サーバ５の通信制御部２７は、この要求を受信し（ステップ５１）、ユーザの認証をした後、参照・登録権判定部２５は参照・登録権テーブル２３を参照して要求されたデータの登録が妥当か否かを判定する（ステップ５２）。要求が妥当であれば、部門鍵アクセス部２６を介して指定された機密区分に対応する公開部門鍵２２１を取り出して端末装置３へ送信する（ステップ５３）。データ鍵暗号化部１５は、通信制御部１９を介してこの公開部門鍵２２１を受信し（ステップ３５）、データ鍵ＥＫをこの公開部門鍵２２１によって暗号化する（ステップ３６）。次にデータ暗号化部１４及びデータ鍵暗号化部１５は、それぞれ暗号化されたデータＤＴ（ＥＫ）及び暗号化されたデータ鍵ＥＫ（ＤＰ）を通信制御部１９を介してサーバ５へ送信する（ステップ３７）。通信制御部２７は、このデータ及びデータ鍵を受信し、データ及びデータ鍵アクセス部２４を介してそれぞれデータ２１１及びデータ鍵２１２として両者を対応づけて記憶装置２１に格納する（ステップ５４）。

【００１４】図３ａ及び図３ｂは、サーバ５に格納されたデータを参照するときの端末装置３、サーバ５及び鍵管理装置８の処理の流れを示すフローチャートである。端末装置３の入出力部１２は、対象となるデータの名称、例えばファイル名を入力し、通信制御部１９を介してサーバ５へデータ要求を送信する（ステップ４１）。サーバ５の通信制御部２７は、この要求を受信し（ステップ６１）、ユーザの認証をした後、参照・登録権判定部２５は、参照・登録権テーブル２３を参照して要求されたデータの参照が妥当か否かを判定する（ステップ６２）。要求が妥当であれば、データ鍵アクセス部２４は、指定されたデータ２１１と対応するデータ鍵２１２とを送信する（ステップ６３）。入出力部１２は、このデータ２１１及びデータ鍵２１２を受信し（ステップ４２）、個人鍵アクセス部１６を介して公開個人鍵１１１を取り出し（ステップ４３）、この公開個人鍵１１１及び受信したデータ鍵２１２を通信制御部１９を介してサ

一バ５へ送信する（ステップ４４）。通信制御部２７はこの公開個人鍵１１１及びデータ鍵２１２を受信し（ステップ６４）、部門鍵アクセス部２６は秘密部門鍵２２２を取り出して（ステップ６５）、端末装置３から受け取った公開個人鍵１１１とデータ鍵２１２並びに取り出した秘密部門鍵２２２を通信制御部２７を介して鍵管理装置８へ送信する（ステップ６６）。鍵管理装置８の秘密部門鍵復号部７３は、通信制御部７５を介してこれらの情報を受信し（ステップ８１）、マスタ鍵アクセス部７２を介して秘密マスタ鍵７１２を取り出し（ステップ８２）、秘密マスタ鍵７１２によって秘密部門鍵２２２を復号し（ステップ８３）、復号された秘密部門鍵ＤＳでデータ鍵２１２を復号する（ステップ８４）。次にデータ鍵暗号化部７４は、公開個人鍵１１１によって得られたデータ鍵ＥＫを暗号化し（ステップ８５）、通信制御部７５を介してサーバ５へこのデータ鍵ＥＫ（ＰＰ）を送信する（ステップ８６）。通信制御部２７はこのデータ鍵を受信し（ステップ６７）、端末装置３へ転送する（ステップ６８）。端末装置３のデータ鍵復号部１７は、通信制御部１９を介してこのデータ鍵ＥＫ（ＰＰ）を受信し（ステップ４５）、個人鍵アクセス部１６を介して秘密個人鍵１１２を取り出し（ステップ４６）、データ鍵ＥＫ（ＰＰ）を秘密個人鍵１１２によって復号する（ステップ４７）。次にデータ復号部１８は得られたデータ鍵ＥＫによって先に受信したデータ２１１を復号し（ステップ４８）、入出力部１２が復号されたデータを出力装置に出力する（ステップ４９）。

【００１５】図４は、データ２１１、データ鍵２１２と機密区分との関連を説明する図である。機密区分は、レベル１，レベル２，・・・のように区分される。機密区分の各レベルは、後述するようにユーザのグループと関連付けられており、各ユーザグループは参照・登録権テーブル２３に登録されているレベルの部門鍵しか利用できない。データ鍵によって暗号化されたデータ２１１は、機密区分とは独立である。公開部門鍵２２１及び秘密部門鍵２２２は、それぞれ機密区分のレベルに対応して設定されるので、公開部門鍵２２１によって暗号化され、秘密部門鍵２２２によって復号されるデータ鍵２１２は、機密区分のいずれかのレベルに対応して登録される。

【００１６】図５は、データの参照又は登録に先立って行うユーザの認証処理の例を説明する図である。サーバ５は、各ユーザのユーザ名とパスワードとの対応テーブル、認証用公開鍵及び認証用秘密鍵を記憶装置に保持する。端末装置３は入力されたユーザ名（ユーザコード）をサーバ５へ送信する。サーバ５の図示しない認証処理部は、このテーブルを参照してユーザ名が登録してあれば、認証用公開鍵ＩＰを端末装置３へ送信する。端末装置３は入力されたパスワードをこの認証用公開鍵で暗号化してサーバ５へ送る。サーバ５は、暗号化されたパスワードＰＷＡ（ＩＰ）を認証用秘密鍵ＩＳで復号してパスワードＰＷＡを得て、テーブル上のユーザ名Ａに対応するパスワードＰＷＡと照合する。パスワードが一致すれば、サーバ５は操作を許可するメッセージを端末装置３へ送信し、端末装置３はデータの参照又は登録の要求を送信する。なお認証用公開鍵及び認証用秘密鍵は適当な頻度で新しい鍵に変更されるものとする。

【００１７】図６は、参照・登録権判定部２５が行うデータの参照権及び登録権を判定する処理の具体例を説明する図である。ユーザの認証処理に使用されるユーザ名とパスワードの対応テーブルは、各ユーザごとにそのユーザの属するユーザグループの識別子を保持している。また参照・登録権テーブル２３は、各グループごとにデータ参照を許可する機密区分のレベルとデータ登録を許可する機密区分のレベルとを設定する。データ登録権のあるユーザはそのデータを更新することもできる。例えばユーザ名Ａのユーザは、ユーザグループＧ１に属するので、機密区分がレベル１のデータしか参照できない。また機密区分がレベル１のデータしか登録できない。またデータ鍵の機密区分を変更する場合には、ユーザは変更前のデータの参照権と変更後のデータの登録権を必要とする。例えば機密区分をレベル１からレベル２に変更する場合には、グループＧｐに属するユーザのようにレベル１のデータの参照権とレベル２のデータの登録権が必要である。図６の例において機密区分のレベルｎは、他システムへデータを転送する権限を設定する。従って例えばグループＧｋに属するユーザのようにレベルｎのデータについて登録権のあるユーザのみが他システムへデータを転送できる。

【００１８】上記実施形態によれば、サーバ５に格納されるデータ鍵２１２は機密区分に対応して暗号化されるとともに参照・登録権テーブル２３に従って参照・登録権のチェックを行うので、その機密区分をもったデータについて参照・登録権のあるユーザだけがそのデータを参照・登録できる。特に機密性の高いレベルのデータが機密性の低いレベルのデータに書き換えられることがないように参照・登録権テーブル２３の機密区分のレベルを機密性の程度に応じて設定し、各ユーザグループに許可する機密区分のレベルを制限することによって、機密性の高いデータのセキュリティを強化できる。またユーザはいずれかのユーザグループに属するので、そのユーザグループに対して許可される機密区分をもったデータを共有することができる。データ鍵２１２は機密区分に対応しているが、データ２１１は機密区分から独立しているので、ネットワークを介してデータ２１１を伝送したりデータ２１１を復号することなくデータ鍵ＥＫ（ＤＰ）の機密区分を変更することが可能である。ステップ８４でデータ鍵２１２が復号された後は、データ鍵ＥＫは機密区分から独立となる。そしてステップ８５で公開個人鍵によって暗号化されてネットワークを介して端末

装置３まで伝送されるので、ネットワーク伝送中のデータ鍵ＥＫの盗聴は実質的に無効である。またサーバ５の管理者は秘密マスタ鍵２２２を復号できず、従ってデータ鍵２１２を復号できず、実質的にデータ２１１にアクセスできない。さらに本発明は、オペレーティングシステムに依存せずアプリケーションプログラムのレベルで実現できるので、特定のハードウェアやオペレーティングシステムには依存しないアクセス制御が可能である。

【００１９】図７は、本発明を適用するシステム形態の例を示す図である。システムＡ及びシステムＢは、それぞれ端末装置３，３’、サーバ５，５’及び鍵管理装置８，８’から構成され、システムＡとシステムＢは通信網を介して接続されている。

【００２０】公開部門鍵２２１及び対となる秘密部門鍵２２２を機密区分ごとに設けておくことによってデータ鍵２１２が機密区分の役割を果たし、その機密区分のデータについてアクセス権をもつユーザグループの間でデータを共有できる。またデータＤＴ１（ＥＫ１）に対応するデータ鍵ＥＫ１（ＤＰ１）の公開部門鍵２２１をＤＰ２に変更する場合には、端末装置３から元のデータ鍵２１２と変更後の機密区分とをサーバ５へ送信し、サーバ５は秘密部門鍵ＤＳ１（ＭＰ）、データ鍵ＥＫ１（ＤＰ１）及び公開部門鍵ＤＰ２を鍵管理装置８へ送信し、鍵管理装置８は秘密マスタ鍵ＭＳによって秘密部門鍵ＤＳ１（ＭＰ）を復号しＤＳ１を得る。次にＤＳ１を用いてデータ鍵ＥＫ１（ＤＰ１）を復号しＥＫ１とした後、新たな公開部門鍵ＤＰ２によってデータ鍵ＥＫ１を再度暗号化してデータ鍵ＥＫ１（ＤＰ２）を得る。これを受けたサーバ５は記憶装置２１に格納されるデータ鍵ＥＫ１（ＤＰ１）をデータ鍵ＥＫ１（ＤＰ２）によって更新する。これによってデータＤＴ１（ＥＫ１）を復号することなくデータの機密区分を変更できる。システムＡからシステムＢにデータを伝送する場合も同様にデータ鍵ＥＫ１（ＤＰ１）について上記と同様の手順を実行し他システムＢの公開部門鍵ＤＰ１’によって再暗号化することによって安全に他システムＢへデータを伝送することができる。

【００２１】以上述べたように、データの参照と登録、データの機密区分の変更、他システムへデータ伝送する場合には必ずサーバ５が介入してユーザの認証に続いてデータ操作の権限をチェックするので、権限のない人間が不正にデータを取得したり勝手にデータを配布する操作を防止することができる。またサーバ５から端末装置３へ送信するデータ及びデータ鍵が盗聴されたとしても、データ鍵は公開部門鍵又は公開個人鍵によって暗号化されているので秘密部門鍵又は秘密個人鍵を知らなければ復号できず、従ってデータの機密性を確保できることが理解される。

【００２２】なお上記実施形態では、鍵管理装置８をサーバ５から独立した装置として設けたが、サーバ５側の記憶装置２１、記憶装置２２、データ及びデータ鍵アクセス部２４、参照・登録権判定部２５、部門鍵アクセス部２６と鍵管理装置８の記憶装置７１、マスタ鍵アクセス部７２、秘密部門鍵復号部７３、データ鍵暗号化部７４とが独立した関係に保たれるならば、鍵管理装置８の各処理部及びデータ部をサーバ内に設けてもよい。なおサーバ５の管理者に信頼を置くのであれば、マスタ鍵を設けず秘密部門鍵ＤＳを暗号化しないものとしてもよい。また上記実施形態では１つのサーバ５に対して１台の鍵管理装置８及び１つのマスタ鍵を設けたが、複数のサーバ５と鍵管理装置８の各々について複数のマスタ鍵を設けることも可能である。また複数台のサーバ５に対して１台の鍵管理装置８を設けることも可能である。また本実施形態に示したユーザ認証方式はあくまで一つの例であり、ケルベロス認証等の他の個人認証技術を使うことが可能である。

【００２３】

【発明の効果】以上説明したように本発明によれば、暗号通信技術を用いてユーザグループの間で安全にデータを共有でき、しかも特別なハードウェアやオペレーティングシステムに依存しないアクセス制御を実現できる。

【図面の簡単な説明】

【図１】実施形態のアクセス制御システムの構成図である。

【図２】実施形態のデータ登録時の端末装置３及びサーバ５の処理の流れを示すフローチャートである。

【図３ａ】実施形態のデータ参照時の端末装置３及びサーバ５の処理の流れを示すフローチャートである。

【図３ｂ】実施形態のデータ参照時の鍵管理装置８の処理の流れを示すフローチャートである。

【図４】データ、データ鍵及び機密区分の関連を説明する図である。

【図５】ユーザ認証処理の例を説明する図である。

【図６】実施形態のデータの参照権及び登録権を判定する処理を説明する図である。

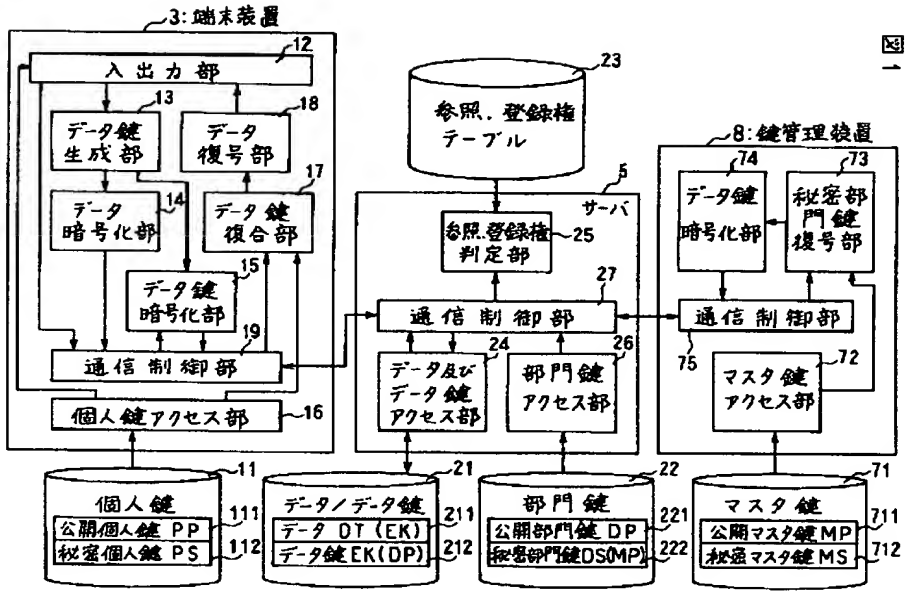
【図７】本発明を適用するシステム形態の例を示す図である。

【図８】従来の暗号通信システムの構成を示す図である。

【符号の説明】

３：端末装置、５：サーバ、８：鍵管理装置、１３：データ鍵生成部、１４：データ暗号化部、１５：データ鍵暗号化部、１７：データ鍵復号部、１８：データ復号部、２３：参照・登録権テーブル、２５：参照・登録権判定部、７３：秘密部門鍵復号部、７４：データ鍵暗号化部、１１１：公開個人鍵、１１２：秘密個人鍵、２１１：データ、２１２：データ鍵、２２１：公開部門鍵、２２２：秘密部門鍵、７１１：公開マスタ鍵、７１２：秘密マスタ鍵

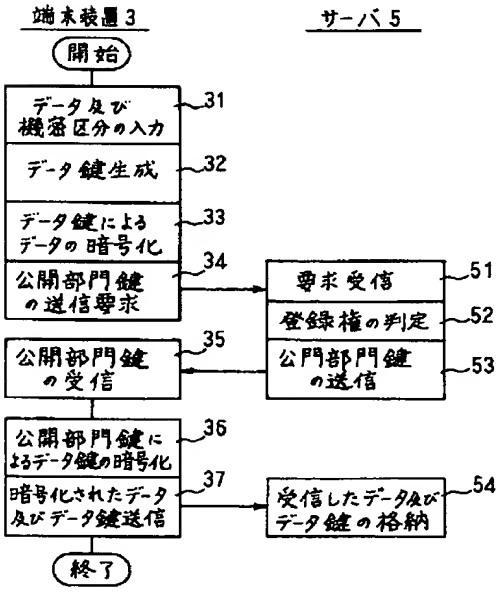
【図１】




図一

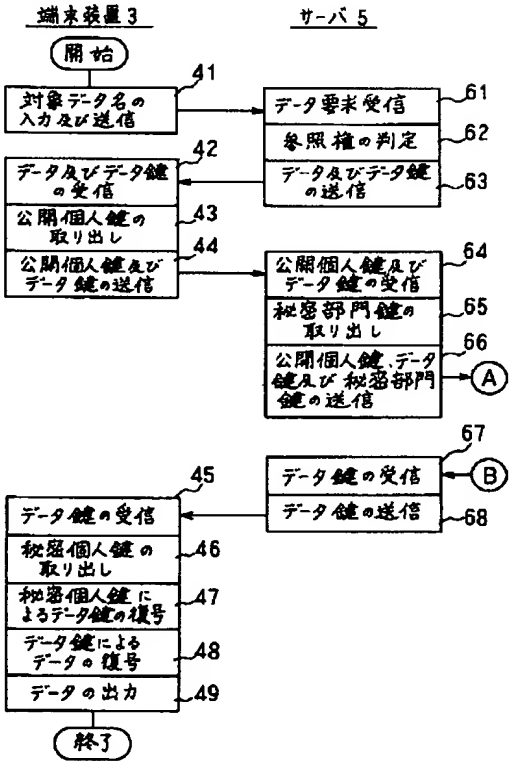
【図２】

図 2



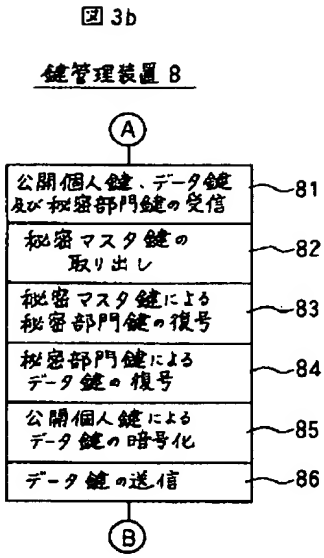

【図３ａ】

図 3a




【図３ｂ】

図 3b



【図４】

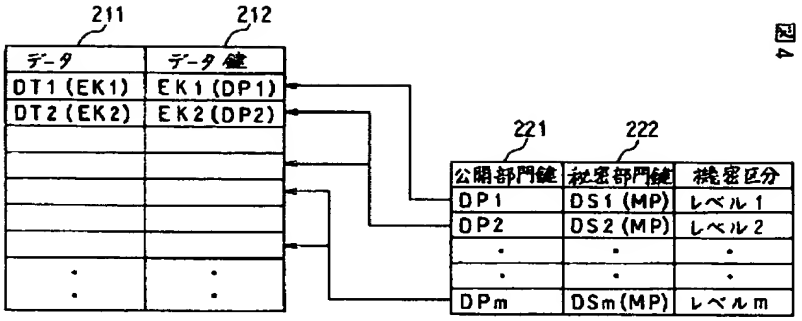



図4

【図５】

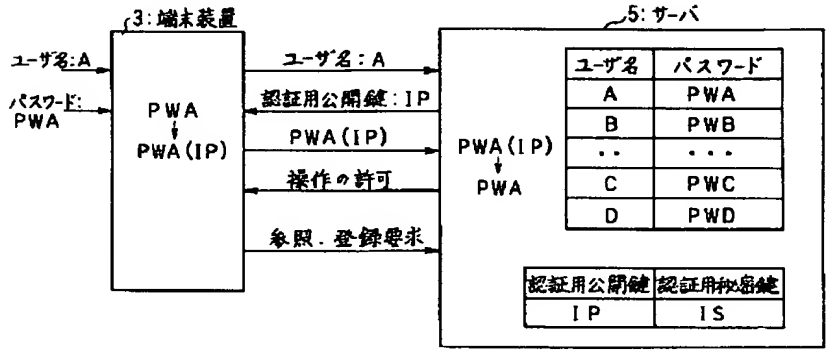



図5

【図６】

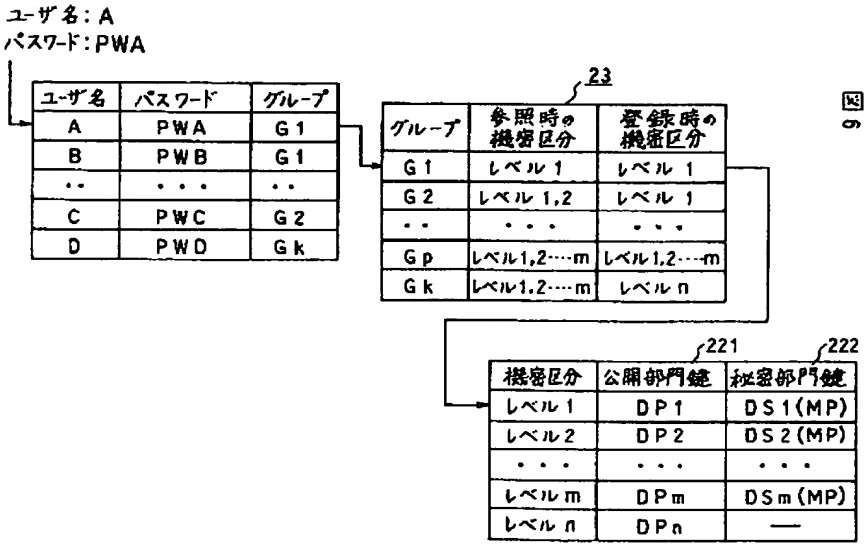
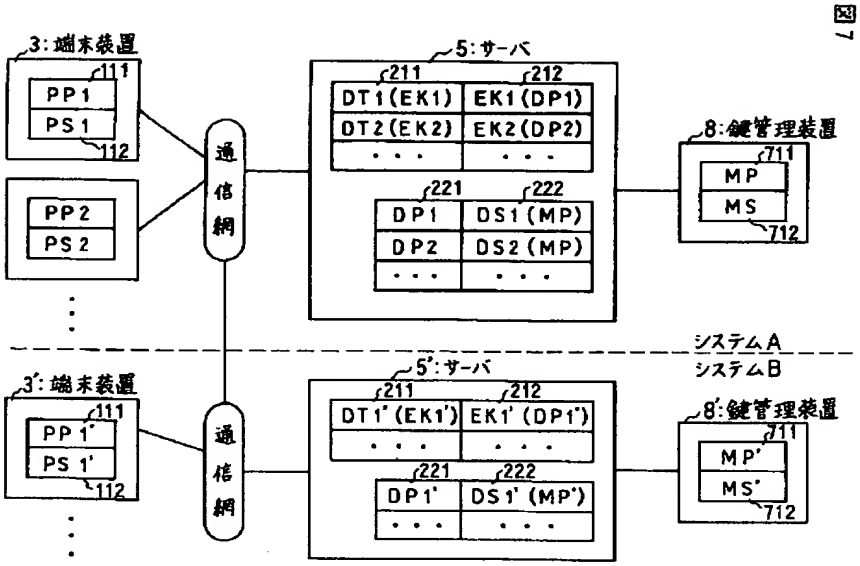
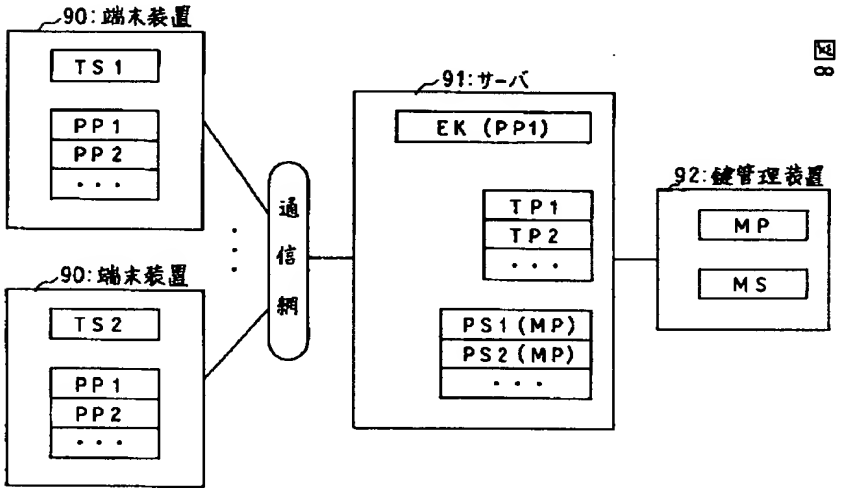



図6

【図７】




【図８】




---

フロントページの続き

(72)発明者　宝木　和夫
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(72)発明者　柴原　節男
東京都江東区新砂一丁目６番27号　株式会社日立製作所公共情報事業部内